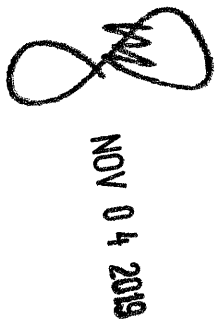
IN THE UNITED STATES DISTRICT COURT

FOR THE DISTRICT OF ALASKA

IN THE MATTER OF THE SEARCH OF a black Alcatel cellular telephone CURRENTLY LOCATED IN the Bureau of Alcohol, Tobacco, Firearms and Explosives Evidence Vault identified as ATF Item #: 000006	Case No. 3:19-mj-00510-MMS



AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER RULE 41 FOR A WARRANT TO SEARCH AND SEIZE

I, Sarah L. Foreman, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1) I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property – a black Alcatel cellular telephone that is currently in possession of the Bureau of Alcohol, Tobacco, Firearms and Explosives and is identified as ATF Item #: 000006, and the extraction from that property of electronically stored information described in Attachment B.

2) I am a Special Agent for the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF) and have been so employed since October 2009. As a Special Agent for the Bureau of ATF, I have completed the Criminal Investigator Training Program at the Federal Law Enforcement Training Center in Glynco, Georgia and Special Agent Basic Training for the ATF. Additionally, I have a Master's Degree in Public Administration with emphasis on Criminal Justice.

3) This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

IDENTIFICATION OF THE DEVICE TO BE EXAMINED

4) The property to be searched is identified as ATF Item #: 000006, a black Alcatel cellular telephone, hereinafter the "Device." The Device is currently located at the ATF Evidence Vault.

PROBABLE CAUSE

5) October 31, 2019 the United States Marshal Service Fugitive Task Force located and arrested Mikeylee Borja MUNA on a Bureau of Prisons Arrest Warrant. MUNA was the sole occupant of a 1997 Honda Integra bearing Alaska License Plate: JNP736 parked in the driveway of 3745 W. 64th Avenue, Anchorage, AK 99502. During his arrest law enforcement recovered a pistol, Ruger, Model: Mark II Target, Cal: .22, Serial #: 215-43878 with a sawed off barrel in his jacket pocket. The firearm was not in a holster, a round was chambered and three additional rounds in the magazine. A check in NCIC shows the firearm was reported as stolen.

6) In plain view in the Honda Integra bearing Alaska License Plate: JNP736 was a pistol grip shotgun propped up on the front passenger seat, accessible to the driver. Additionally, boxes of ammunition were observed on the passenger seat and floorboard. The shotgun was seized plain view and the vehicle seized pending application of a search warrant. The shotgun was identified as a Mossberg, Model: 500A, Caliber: 12 Gauge, Serial #: R810060, loaded with five (5) rounds in the magazine tube. This firearm was not reported stolen in NCIC.

7) SA Foreman ran a criminal history on Mikeylee Borja MUNA, DOB: 08/05/1981, FBI#: 235051JB8 and found MUNA has the following felony convictions:

i. State of Alaska Case: 3PA-11-2998CR convicted on January 20, 2012 of Assault 3 Domestic Violence

ii. United State District Court – District of Alaska Case: 3:13-cr-00100-01-SLG convicted of two counts of Felon in Possession on February 11, 2014.

8) A search of the Bureau of Prisons Inmate Locator (www.bop.gov) lists MUNA as escaped on September 12, 2019.

9) November 1, 2019 SA Foreman applied for and was granted Federal search warrant 3:19-mj-00503-MMS for the search of the 1997 Honda Integra bearing Alaska License Plate: JNP736. During the execution of the search warrant, four cellular telephones and one tablet were seized from the vehicle.

10) Based upon my training and experience it is common for the following:

i. Individuals who cannot lawfully purchase firearms typically utilize cellular telephones and other mobile communication devices to obtain firearms through individuals without Federal Firearms Licenses to avoid background checks.

ii. Individuals who cannot lawfully purchase firearms may utilize cellular telephones and other mobile communication devices to make contact with non-prohibited individuals to coordinate the straw-purchase of firearms.

iii. Individuals who illegally possess firearms to document their activities, most easily via cellular telephones and other mobile communication devices as they are capable of photographing and recording video, as well as then sharing the documentation on various media platforms. I also know people use the internet, most readily available on most cellular devices, to browse and research firearms and ammunition.

iv. Individuals utilize cellular telephones and other mobile communication devices to take, maintain, send and receive photographs, including those of firearms and of themselves possessing said firearms.

v. Records of such contacts, whether call logs or text messages, are frequently maintained in the cellular telephone's memory.

vi. It is common for individuals involved in illegal activities to use multiple cellular telephones to maintain contact with their associates. These individuals use multiple cellular telephones because cellular telephones are mobile and can be easily obtained with a different subscriber name.

vii. It is common for individual to take or cause to be taken, photographs and/or videos of themselves, firearms, and/or their co-conspirators and associates. The aforementioned images are frequently maintained in the memory of cellular telephone devices. Devices such as smart cellular telephones often imprint each photo with the GPS coordinates where such photos are taken. Thus, it is possible the location of illegal firearm possession/transactions and other evidence by analyzing a digital photo.

viii. Certain cellular telephones have a feature which allow the subscriber or user of the device remote access to "wipe" or delete all the information if the device no longer in their possession whether it be because it is lost, stolen, or seized.

TECHNICAL TERMS

11) Based on my training, and experience, I know cellular telephones often have capabilities that allow them to serve as a wireless telephone, digital camera, portable media player, GPS navigation device, PDA, and to access the Internet. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device.

12) Based on my training and experience, I use the above technical terms to convey the following meanings:

a. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving, and

NOV 04 2019

storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the device.

b. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.

c. Portable media player: A portable media player (or "MP3 Player" or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.

d. GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another

NOV 0 4 2019

location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated "GPS") consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna's latitude, longitude, and sometimes altitude with a high level of precision.

e. PDA: A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments or notes) and utilizing computer programs. Some PDAs also function as wireless communication devices and are used to access the Internet and send and receive e-mail. PDAs usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer software, giving them many of the same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets, and presentations. PDAs may also include global positioning system ("GPS") technology for determining the location of the device.

f. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

NOV 04 2019

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

13) Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

14) There is probable cause to believe that things that were once stored on the Device may still be stored there, for at least the following reasons:

- Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.
- Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.
- Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is

NOV 04 2019

typically required for that task. However, it is technically possible to delete this information.

- Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

15) *Forensic evidence.* As further described in Attachment A, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the Device was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the Device because:

- Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).
- Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.
- A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.
- The process of identifying the exact electronically stored information on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

NOV 04 2019

- Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

16) *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the device consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

17) *Manner of execution.* Because this warrant seeks only permission to examine a device already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premise. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

NOV 0 4 2019

CONCLUSION

Based upon the foregoing, your affiant submits this affidavit as probable cause to believe Mikeylee MUNA is in violation of Title 18 U.S.C. §922(g)(1) that persons convicted of a felony in which the punishment exceeds one year are prohibited from possessing a firearm or ammunition, as defined by Title 18, United States Code, Section 921(a), which have traveled in and affected interstate commerce and is requesting a search warrant be granted authorizing the examination of the Device identified as a black Alcatel cellular telephone that is currently in possession of the ATF and is identified as ATF Item #: 000006 to seek the items described in Attachment B.

Respectfully submitted,

Sarah L. Foreman
Special Agent
Bureau of Alcohol, Tobacco, Firearms and Explosives

Subscribed and sworn to before me
on November 4, 2019:

UNITED STATES MAGISTRATE JUDGE

UNITED STATES DISTRICT COURT
DISTRICT OF ALASKA